Functional Privacy
or Why Cookies are Better with Milk

Robert J. Walls  Shane S. Clark  Brian N. Levine

Department of Computer Science
University of Massachusetts Amherst

This work was supported in part by a National Science Foundation Graduate Research Fellowship and in part by a grant from the UMass President's Office.

rjwalls@cs.umass.edu
Functional Privacy
double click
Collusion Demo

Thanks for trying out this demo. If you'd like to see this graph change in real time based on the sites you visit in your own browser, feel free to try the Collusion Firefox add-on. Even visiting the sites mentioned in the demo will probably give you different visualizations, because some services you may be logged into—like Facebook—can also track you across sites.

If you want to block companies from tracking you on the internet, you can install TrackerBlock for Firefox and Internet Explorer.

Collusion was created as a prototype by Atul Varma. For more information about the making of this demo, check out the
“If you are not paying for it, you're not the customer; you're the product being sold.”

-Andrew Lewis
How do we help the common user?
User’s dilemma:
privacy with reduced functionality versus full functionality without privacy.
User’s dilemma: privacy with reduced functionality versus full functionality without privacy.

Intuition: When forced to choose, most users will pick functionality over privacy.
Functional privacy: The privacy that can be obtained without a reduction in service.

Privacy tools will often better serve the common user by adopting a functional privacy approach.
Functional privacy: The privacy that can be obtained without a reduction in service.

Privacy tools will often better serve the common user by adopting a functional privacy approach.
Milk:

A functional privacy approach for limiting consumer tracking on the web.

Implemented as a Chrome extension.
Cookie Binding

Key concept: bind each cookie to the domain that sets it.
Key concept: bind each cookie to the domain that sets it.
Key concept: bind each cookie to the domain that sets it.
Key concept: bind each cookie to the domain that sets it.
Key concept: bind each cookie to the domain that sets it.
Key concept: bind each cookie to the domain that sets it.
Cookie Binding

Key concept: bind each cookie to the domain that sets it.
Key concept: bind each cookie to the domain that sets it.
**Cookie Binding**

Key concept: bind each cookie to the domain that sets it.
Cookie Binding

Key concept: bind each cookie to the domain that sets it.
Milk Example

Key concept: third-party tracking cookies are not shared across domains.
Key concept: third-party tracking cookies are not shared across domains.
Key concept: third-party tracking cookies are not shared across domains.
Milk Example

Key concept: third-party tracking cookies are not shared across domains.
Milk Example

Key concept: third-party tracking cookies are not shared across domains.
Key concept: third-party tracking cookies are not shared across domains.
Key concept: third-party tracking cookies are not shared across domains.
Milk Example

Key concept: third-party tracking cookies are not shared across domains.
Milk Example

Key concept: third-party tracking cookies are not shared across domains.
Key concept: root cookies are shared across domains.
Key concept: root cookies are shared across domains.
Key concept: root cookies are shared across domains.
Milk Root Store

Key concept: root cookies are shared across domains.
Key concept: root cookies are shared across domains.
Key concept: root cookies are shared across domains.
Milk Limitations

• Proof of concept, not a product.

• Other tracking methods besides cookies, e.g. IP address, HTML 5 local storage.

• Chrome lacks a synchronous Cookie API.
Tools on the web:

- ShareMeNot [Roesner, NDSI 2012]
- HTTPS Everywhere
- User-Agent Entropy

Other domains:

- Privacy-preserving toll systems
- Location-based services
- Cell phone IMEI tracking
Not all functionally private solutions are effective.

- Informed consent
- Do Not Track headers
Informed Consent

• **Idea:** Give the user information about how their information is used.

• **Problem:** ???
PANDORA MEDIA, INC.
TERMS OF USE
(EFFECTIVE AS OF NOVEMBER 15, 2011)

PLEASE READ CAREFULLY

Should you have any questions concerning this Agreement or need technical support, you may contact Pandora support by visiting http://help.pandora.com.

This Pandora Media, Inc. Terms of Use Agreement (this "Agreement") is a legal agreement between you and Pandora Media, Inc. and its subsidiaries ("Pandora", "we", "us" or "our") providing, among other things, the terms and conditions for your use of Pandora’s streaming music and content services (collectively, the "Pandora Services"), including but not limited to delivery via our Web site [http://www.pandora.com] (the "Site"), a mobile device, or otherwise.

We may from time to time modify these terms of use and will post a copy of the amended Agreement at http://help.pandora.com.

You may use the Services only if you can form a binding contract with Twitter and are not a person barred from using the Services, including by reason of any applicable age restriction. If you are acting on behalf of an account from which you are currently logging in, you represent that you have the authority to agree to these terms.

Read Pandora’s Privacy Policy

To make it a bit easier to digest our Terms of Use, we thought we’d start by highlighting in plain English some of the issues. This summary is not a legal document. Of course you’ll want to read the complete Terms of Use, but here is what we think is important:

Terms:

- You must be at least 13 years old to open a Pandora account. Pandora can only be used in certain countries.
- We expect you to keep your account password to yourself.
- Except as set forth below in Section 2.1, Pandora is for personal use only. That means you can’t play Pandora for the patrons in your bar, coffee shop, etc.
- You can’t use Pandora to steal music or other content, and you have to listen to it through pandora.com or on a device officially supported by Pandora.
- Do not use Pandora if you do not agree to the Terms of Use. Your use of Pandora means you agree to the Terms of Use.
Informed Consent

- **Idea**: Give the user information about how their information is used.

- **Problem**: Too much to read, too hard to understand, too little time --- about 200 hours worth of reading per year.
Do Not Track

- **Idea:** Header mechanism for opting out.
- **Problem:** ???
Conflict Over How Open ‘Do Not Track’ Talks Will Be

By EDWARD WYATT and TANZINA VEGA
Published: March 30, 2012

WASHINGTON — Technology companies want to talk with the government about protecting privacy on the Internet. They just want those talks to be private.

Representatives of advertising companies, Internet sites and technology companies told a House subcommittee on Thursday that they thought Internet privacy policies, including Do Not Track options, should be created through an “open and transparent” process, as two government agencies have recommended.

But openness is relative. “If this process takes the form of a public discussion, industry participants will be looking over their shoulders or sitting on their hands instead of offering bold ideas for workable solutions,” said Jonathan Zuck, president of the Association for Competitive Technology, a trade association of software, hardware and technology consulting companies.

The Commerce Department and the Federal Trade Commission, which are encouraging companies to be more open with consumers about their privacy policies, say that any such talks should be accessible to, if not include, Internet users.

“We don’t think there is any substitute for openness and transparency,” Lawrence E. Strickling, assistant secretary for communication and information at the Commerce Department, told the subcommittee, a part of the House Energy and Commerce Committee.
“The advertising group, however, defines it as forbidding the serving of targeted ads to individuals but not prohibiting the collection of data.”
Do Not Track

- **Idea**: Header mechanism for opting out.
- **Problem**: Little incentive for companies to provide privacy.
Conclusions

- Functional privacy is the privacy that can be obtained without a reduction in service.
- Privacy tools will often better serve the common user by adopting a functional privacy approach.

Milk is available at [http://forensics.umass.edu/milk.php](http://forensics.umass.edu/milk.php)